PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-182770
(43)Date of publication of application : 26.06.2002

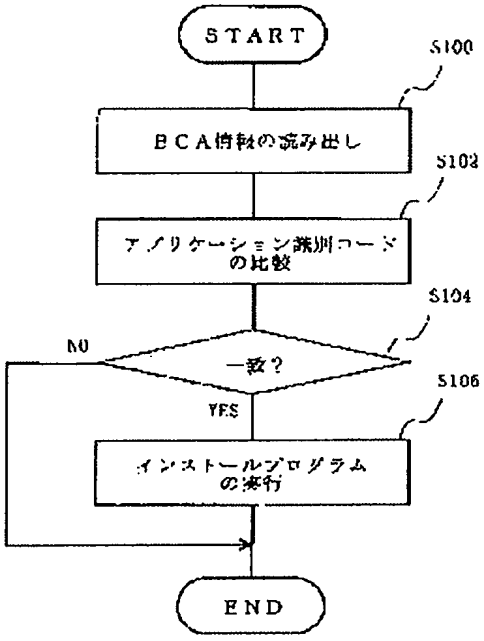
(51)Int.Cl. G06F 1/00
G06F 12/14
H04L 9/32

(21)Application number : 2000-384209
(22)Date of filing : 18.12.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MORIYAMA YUKICHI
NISHII KIYOSHI

(54) RECORDING MEDIUM HAVING NORMAL USER AUTHENTICATION FUNCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a recording medium capable of simplifying the authentication work of normal user and also preventing an illegal use by an illegal copy.
SOLUTION: First, identification information in a BCA area is read according to a normal user authentication program (S100). An application identification code included in the read identification information is compared with a normal application identification code described in the authentication program (S102), and whether or not the codes coincide with each other is judged (S103). When the codes coincide, the user of the read identification information is judged to be a normal user allowed to use the original disk, a software program is installed according to an install program (S104) and the processing is finished. Meanwhile, when the codes do not coincide, the user is judged to be an illegal user, the processing is finished without conducting the install program.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－182770
（P2002－182770A）
(43)公開日　平成14年６月26日(2002.6.26)

(51)Int.Cl.'	識別記号	Ｆ１		テーマコード'（参考）
Ｇ０６Ｆ　1/00		Ｇ０６Ｆ　12/14	３２０Ａ	５Ｂ０１７
12/14	３２０	9/06	６６０Ｅ	５Ｂ０７６
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｊ１０４

審査請求　未請求　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願2000－384209(P2000－384209)

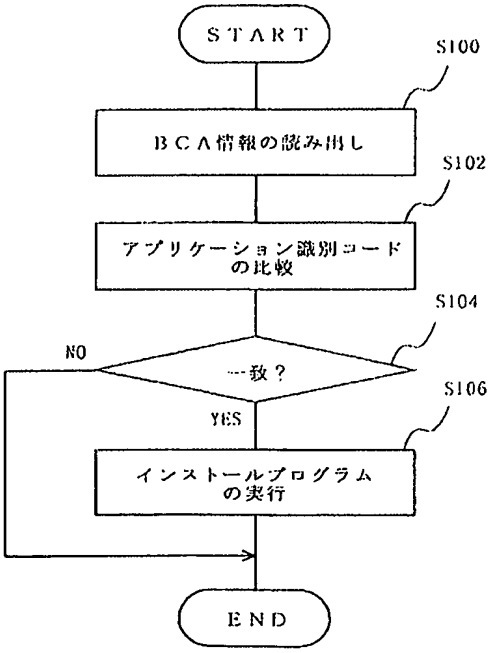
(22)出願日　平成12年12月18日(2000.12.18)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　森山　諭吉
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　西井　清
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100098291
弁理士　小笠原　史朗

Ｆターム(参考)　5B017 AA07 BA07 CA15
5B076 FA20 FB05
5J104 AA07 KA01 NA05 NA32 PA14

(54)【発明の名称】　正規ユーザ認証機能付き記録媒体

(57)【要約】
【課題】　ソフトウエアプログラムの不正コピーを防止するために手作業によりＣＤキーの入力を行うのは手間であり、不正防止に対する有効性にも欠ける。
【解決手段】　正規ユーザ認証プログラムに従って、まずＢＣＡ領域の識別情報を読み出す（Ｓ１００）。そして、読み出した識別情報に含まれるアプリケーション識別コードと認証プログラムに記述されている正規のアプリケーション識別コードとを比較し（Ｓ１０２）、それらコードが一致するか否かを判定する（Ｓ１０３）。一致する場合にはオリジナルのディスクを使用する正規のユーザであると判断してインストールプログラムに従ってソフトウエアプログラムのインストールを実行し（Ｓ１０４）、処理を終了する。一方、一致しない場合には、不正なユーザであると判断してインストールプログラムを実行することなく処理を終了する。



1

【特許請求の範囲】
【請求項１】　コンテンツ読み出し端末にコンテンツを供給するためのコンピュータ読み取り可能な記録媒体であって、
前記コンテンツ及び所定のプログラムを格納するデータ格納領域と、
所定の固有情報を格納する書き換え不可能な領域とを備え、
前記所定のプログラムは、
前記コンテンツ読み出し端末に、
前記所定の固有情報を読み出すステップと、
当該読み出した所定の固有情報に基づいて正規ユーザの認証を行う認証ステップと、
前記認証ステップの認証結果に応じて前記コンテンツを有効化する有効化ステップとを実行させるためのプログラムであることを特徴とする、正規ユーザ認証機能付き記録媒体。
【請求項２】　前記書き換え不可領域がＤＶＤのＢＣＡ領域（ＢｕｒｓｔＣｕｔｔｉｎｇ　Ａｒｅａ）であることを特徴とする、請求項１記載の正規ユーザ認証機能付き記録媒体。
【請求項３】　前記コンテンツがソフトウエアプログラムであり、
前記有効化ステップは前記認証ステップの認証結果に応じて当該ソフトウエアプログラムをインストールすることを特徴とする、請求項１記載の正規ユーザ認証機能付き記録媒体。
【請求項４】　前記コンテンツが前記データ格納領域に暗号化して格納されており、
前記有効化ステップは前記認証ステップの認証結果に応じて当該暗号化されたコンテンツを復号化することを特徴とする、請求項１記載の正規ユーザ認証機能付き記録媒体。
【請求項５】　前記所定の固有情報は前記コンテンツを識別するためのコンテンツ識別コードを含み、
前記認証ステップは前記コンテンツ識別コードが正規のコンテンツ識別コードに一致するか否かを判断することによって正規ユーザの認証を行うことを特徴とする、請求項１記載の正規ユーザ認証機能付き記録媒体。
【請求項６】　前記所定の固有情報はチェックデジットを含み、
前記認証ステップは前記固有情報に基づいて所定の演算を実行した結果が前記チェックデジットに一致するか否かを判断することによって正規ユーザの認証を行うことを特徴とする、請求項１記載の正規ユーザ認証機能付き記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、正規ユーザ認証機能付き記録媒体に関し、より特定的には、コンテンツ読み出し端末にコンテンツを供給するためのコンピュータ読み取り可能な記録媒体に関する。

2

【０００２】
【従来の技術】従来、ＣＤ－ＲＯＭに記録されたソフトウエアをインストールして利用する場合、通常、インストール時やインストール後の起動時にＣＤキーの入力が必要となる。このとき、所定のＣＤキーの入力がなければ、ソフトウエアを利用することができない。
【０００３】ＣＤキーは、通常、ＣＤ－ＲＯＭやケースやマニュアルなどに記載されている。したがって、ソフトウエアを記録したＣＤ－ＲＯＭを不正コピーした場合、不正コピーしたメディアを入手したユーザにはＣＤキーが分からない。このため、オリジナルのＣＤ－ＲＯＭを購入した正規のユーザのみがソフトウエアを利用することができる。
【０００４】
【発明が解決しようとする課題】しかしながら、上述の方法では、インストールする際などにユーザがＣＤキーを手作業で入力する手間を要し、また、ＣＤキーを記載したケースやマニュアルについても紛失しないように管理しておく手間を要するという問題がある。
【０００５】さらに、不正コピーしたメディアを入手したユーザがＣＤキーも同時に入手した場合、このユーザによるソフトウエアの不正利用を防止することができないという問題もある。
【０００６】それ故に、本発明の目的は、正規ユーザの認証作業を簡略化でき、かつ不正コピーによる不正利用を防止することのできる記録媒体を提供することである。
【０００７】
【課題を解決するための手段および発明の効果】第１の発明は、コンテンツ読み出し端末にコンテンツを供給するためのコンピュータ読み取り可能な記録媒体であって、前記コンテンツ及び所定のプログラムを格納するデータ格納領域と、所定の固有情報を格納する書き換え不可能な領域とを備え、前記所定のプログラムは、前記コンテンツ読み出し端末に、前記所定の固有情報を読み出すステップと、当該読み出した所定の固有情報に基づいて正規ユーザの認証を行う認証ステップと、前記認証ステップの認証結果に応じて前記コンテンツを有効化する有効化ステップとを実行させるためのプログラムであることを特徴とする。
【０００８】上記のように、第１の発明によれば、書き換え不可能な領域に記録される固有の情報を用いてコンテンツの利用が制限されるため、ユーザがＩＤ等を手作業で入力することなしに認証を行い、オリジナルのメディア以外のメディアに不正コピーされたコンテンツの利用を防止することができる。
【０００９】第２の発明は、第１の発明において、前記書き換え不可領域がＤＶＤのＢＣＡ領域（Ｂｕｒｓｔ

Ｃｕｔｔｉｎｇ　Ａｒｅａ）であることを特徴とする。

【００１０】上記のように、第２の発明によれば、書き換え不可領域として、ＤＶＤに固有のＢＣＡ領域を利用することができる。

【００１１】第３の発明は、第１の発明において、前記コンテンツがソフトウエアプログラムであり、前記有効化ステップは前記認証ステップの認証結果に応じて当該ソフトウエアプログラムをインストールすることを特徴とする。

【００１２】上記のように、第３の発明によれば、認証結果に応じてソフトウエアプログラムのインストールを制限するため、不正コピーによるソフトウエアの不正利用を防止することができる。

【００１３】第４の発明は、第１の発明において、前記コンテンツが前記データ格納領域に暗号化して格納されており、前記有効化ステップは前記認証ステップの認証結果に応じて当該暗号化されたコンテンツを復号化することを特徴とする。

【００１４】上記のように、第４の発明によれば、認証結果に基づいて暗号化済みコンテンツの復号化を制限するため、不正コピーによるソフトウエアの不正利用を防止することができる。

【００１５】第５の発明は、第１の発明において、前記所定の固有情報は前記コンテンツを識別するためのコンテンツ識別コードを含み、前記認証ステップは前記コンテンツ識別コードが正規のコンテンツ識別コードに一致するか否かを判断することによって正規ユーザの認証を行うことを特徴とする。

【００１６】上記のように、第５の発明によれば、コンテンツ識別情報が正規のコンテンツ識別情報と一致するか否かを判断することによって、認証を容易に行うことができる。

【００１７】第６の発明は、第１の発明において、前記所定の固有情報はチェックデジットを含み、前記認証ステップは前記固有情報に基づいて所定の演算を実行した結果が前記チェックデジットに一致するか否かを判断することによって正規ユーザの認証を行うことを特徴とする。

【００１８】上記のように、第６の発明によれば、固有情報に基づく演算結果がチェックデジットに一致するか否かを判断することによって、不正利用をより効果的に防止することができる。

【００１９】

【発明の実施の形態】以下、本発明の種々の実施形態について図面を参照して説明する。

（第１の実施形態）図１は、本発明の第１の実施形態に係るＤＶＤ－ＲＯＭに記録されているソフトウエアプログラムをインストールする際のシステム構成を示すブロック図である。ＤＶＤ－ＲＯＭ１００は、ＤＶＤドライブ３００を介してユーザ端末２００に接続される。ユーザ端末２００のＣＰＵ２１０は、ＤＶＤ－ＲＯＭ１００に記録されているプログラムに従って、ハードディスク２２０にソフトウエアプログラムをインストールする。

【００２０】ＤＶＤ－ＲＯＭ１００は、通常のデータ格納領域の他にＢＣＡ領域（Ｂｕｒｓｔ　Ｃｕｔｔｉｎｇ　Ａｒｅａ）１０を有する。ＢＣＡ領域１０は、製造段階においてディスクの識別情報１１が書き込まれる書き換え不可能な領域である。この識別番号によってディスク毎の識別が可能となる。

【００２１】通常のデータ格納領域には、正規ユーザ認証プログラム１０１、インストールプログラム１０２及びソフトウエアプログラム１０３が格納されている。認証プログラム１０１及びインストールプログラム１０２は、ソフトウエアプログラム１０３をハードディスク２２０にインストールする際にＣＰＵ２１０により実行されるプログラムである。認証プログラム１０１は、このメディア１００が不正コピーされたものではないオリジナルのメディアであるか否かを判別して正規ユーザの認証を行うプログラムである。インストールプログラム１０２は、ソフトウエアプログラム１０３をインストールするためのプログラムである。

【００２２】次に、図２を参照して、ＢＣＡ領域１０に格納される識別情報１１について説明する。本実施形態では、一例として、ＢＣＡ領域１０にはディスクのプレス時に１７０バイトのアプリケーション識別コードと１８バイトのシリアル番号を格納する。アプリケーション識別コードは同一のソフトウエアプログラムに対して共通に与えられる識別コードである。シリアル番号は共通のアプリケーション識別コードを有するグループに対してシリアルに与えられる識別番号である。

【００２３】以下、図３のフローチャートを参照して、ソフトウエアプログラム１０３のインストール時のＣＰＵ２１０の動作について説明する。ＣＰＵ２１０は、正規ユーザ認証プログラム１０１に従って、まずＢＣＡ領域１０の識別情報１１を読み出す（Ｓ１００）。そして、読み出した識別情報１１に含まれるアプリケーション識別コードと認証プログラム１０１に記述されている正規のアプリケーション識別コードとを比較し（Ｓ１０２）、それらコードが一致するか否かを判定する（Ｓ１０３）。一致する場合にはオリジナルのディスクを使用する正規のユーザであると判断してインストールプログラム１０２に従ってソフトウエアプログラム１０３のインストールを実行し（Ｓ１０４）、処理を終了する。一方、一致しない場合には、不正なユーザであると判断してインストールプログラム１０２を実行することなく処理を終了する。

【００２４】次に、以上の動作によって不正コピーによるソフトウエアプログラムの不正利用が防止できることについて説明する。上述したように、ＤＶＤ－ＲＯＭのＢＣＡ領域の情報は、ディスク製造時に記録され、以

後、書き換えることは不可能である。本実施形態に係るＤＶＤ－ＲＯＭ１００には、ディスク製造時に、ＢＣＡ領域１０に所定のアプリケーション識別コードを記録するとともに、正規ユーザ認証プログラム１０１に、このアプリケーション識別コードと同一の正規のアプリケーション識別コードを記述する。したがって、オリジナルのＤＶＤ－ＲＯＭ１００のインストール時には、これらアプリケーション識別コードが一致するため、正常にインストールを実行することができる。

【００２５】一方、このＤＶＤ－ＲＯＭ１００の記録内容が他のメディアに不正コピーされた場合について説明する。例えば、コピー先のメディアがＤＶＤ－ＲＡＭである場合には、このＤＶＤ－ＲＡＭに正規ユーザ認証プログラム１０１、インストールプログラム１０２及びソフトウエアプログラム１０３がコピーされる。しかし、ＢＣＡ領域に格納されている識別情報については書き換え不可能なためコピーされず、コピー先のＤＶＤ－ＲＡＭのＢＣＡ領域にはディスク製造時に記録された識別情報が記録されたままである。したがって、認証プログラム１０１に記述されている正規のアプリケーション識別コードと、ＢＣＡ領域に格納されている識別情報が一致しないため、インストールは失敗に終わる。また、例えば、コピー先のメディアがＣＤ－Ｒである場合には、ＢＣＡ領域そのものがないので、インストールは失敗に終わる。

【００２６】なお、本実施形態では正規ユーザの認証にアプリケーション識別コードを用いたが、これに限らず、例えばＢＣＡ領域内の識別情報全体をキー情報として用いることも可能である。ただし、その場合、ディスク毎にキー情報が異なってしまうため、認識プログラム１０１に記述しておく正規の識別情報も、ディスク毎に変える必要があり、製造時に手間がかかってしまう。したがって、本実施形態のように、シリアル番号を除いた共通の識別コードを認証のためのキー情報として用いるのが製造時の手間を省くという点では好ましい。

【００２７】また、本実施形態では正規ユーザ認証プログラム１０１とインストールプログラム１０２をそれぞれ独立したプログラムとして説明したが、これに限らず、インストールプログラム１０２が認証プログラム１０１の機能を含んでも構わない。

【００２８】また、本実施形態では認証時に用いる正規のアプリケーション識別コードは認証プログラム１０１に記述されているとしたが、これに限らず、ＤＶＤ－ＲＯＭ１００内の他の領域に格納されていても構わない。

【００２９】また、本実施形態ではＤＶＤ－ＲＯＭ１００に記録されるソフトウエアプログラム１０３は１つであるが、複数のソフトウエアプログラムを記録しても構わない。

【００３０】以上のように、第１の実施形態によれば、インストール時等にＣＤキー等を手作業で入力することなしに正規ユーザの認証を行うことができるためインストール作業が簡略化され、さらに、認証のためのキー情報として、書き換え不可能なＢＣＡ領域内の情報を利用しているため、不正コピーによるソフトウエアプログラムの不正利用を防止することができる。

【００３１】（第２の実施形態）図４は、本発明の第２の実施形態に係るＤＶＤ－ＲＯＭに記録されているソフトウエアプログラムをインストールする際のシステム構成を示すブロック図である。図４において、図１と同一の構成には同一の参照符号を付す。

【００３２】第２の実施形態が第１の実施形態と異なる点は、ＢＣＡ領域４０内の識別情報４１と、通常のデータ格納領域内の正規ユーザ認証プログラム４０１のみであるので、以下、これら相違点のみを説明する。

【００３３】次に、図５を参照して、ＢＣＡ領域４０に格納される識別情報４１について説明する。本実施形態では、一例として、ＢＣＡ領域４０にはディスクのプレス時に１６８バイトのアプリケーション識別コードと１８バイトのシリアル番号と２バイトのチェックデジットとを格納する。チェックデジットは、正規ユーザの認証を行う際に用いられる情報である。

【００３４】以下、図６のフローチャートを参照して、ソフトウエアプログラム１０３のインストール時のＣＰＵ２１０の動作について説明する。ＣＰＵ２１０は、正規ユーザ認証プログラム４０１に従って、まずＢＣＡ領域４０の識別情報４１を読み出す（Ｓ２００）。そして、読み出した識別情報４１に含まれるアプリケーション識別コード及びシリアル番号の合わせて１８６バイトの情報に基づいて、認証プログラム４０１に記述されている演算を実行する（Ｓ２０２）。演算結果をチェックデジットと比較し（Ｓ２０４）、それらが一致するか否かを判定する（Ｓ２０６）。一致する場合にはオリジナルのディスクを使用する正規のユーザであると判断して、インストールプログラム１０２に従ってソフトウエアプログラム１０３のインストールを実行し（Ｓ２０８）、処理を終了する。一方、一致しない場合には、不正なユーザであると判断してインストールプログラム１０２を実行することなく処理を終了する。

【００３５】次に、以上の動作によってソフトウエアプログラムの不正コピーによる不正利用が防止できることについて説明する。上述したように、ＤＶＤ－ＲＯＭのＢＣＡ領域の情報は、ディスク製造時に記録され、以後、書き換えることは不可能である。本実施形態に係るＤＶＤ－ＲＯＭ４００には、ディスク製造時に、ＢＣＡ領域４０に所定のアプリケーション識別コード及びシリアル番号を記録するとともに、これらの情報に基づいて所定の演算を行った結果をチェックデジットとして記録し、正規ユーザ認証プログラム４０１に、この所定の演算方法を記述する。したがって、オリジナルのＤＶＤ－ＲＯＭ４００のインストール時には、ＢＣＡ情報に基づ

く演算結果とチェックデジットが一致するため、インストールを実行することができる。

【００３６】一方、このＤＶＤ－ＲＯＭ４００の記録内容が他のメディアに不正コピーされた場合については、コピー先のメディアに正規ユーザ認証プログラム４０１、インストールプログラム１０２及びソフトウエアプログラム１０３がコピーされる。しかし、ＢＣＡ領域に格納されている識別情報については書き換え不可能なためコピーされない。したがって、コピー先のメディアのＢＣＡ領域に格納されている識別情報に基づいて行われる認証プログラム４０１に記述されている演算の結果は識別情報内のチェックデジットと一致しないため、インストールは失敗に終わる。またコピー先のメディアにＢＣＡ領域がない場合にもインストールは失敗に終わる。

【００３７】なお、本実施形態ではアプリケーション識別コード及びシリアル番号に基づいて演算を行ったが、これに限らず、例えばアプリケーション識別コード及びシリアル番号の一部を利用するとしても構わない。

【００３８】また、本実施形態では、第１の実施形態と同様に、インストールプログラム１０２が認証プログラム１０１の機能を含んでも構わない。また、演算方法に関する情報は認証プログラム４０１に記述されているとしたが、ＤＶＤ－ＲＯＭ４００内の他の領域に格納されていても構わない。

【００３９】また、本実施形態ではＤＶＤ－ＲＯＭ４００に記録されるソフトウエアプログラム１０３は１つであるが、複数のソフトウエアプログラムを記録しても構わない。

【００４０】以上のように、第２の実施形態によれば、インストール時等にＣＤキー等を手作業で入力することなしに正規ユーザの認証を行うことができるためインストール作業が簡略化され、さらに、認証のためのキー情報として、書き換え不可能なＢＣＡ領域内の情報を利用しているため、不正コピーによるソフトウエアプログラムの不正利用を防止することができる。そしてさらに、ＢＣＡ領域内の識別情報に基づいて演算を行ってから認証を行うので、不正をより確実に防止することができる。

【００４１】（第３の実施形態）図７は、本発明の第３の実施形態に係るＤＶＤ－ＲＯＭに記録されている映像コンテンツを再生する際のシステム構成を示すブロック図である。ＤＶＤ－ＲＯＭ５００は、ＤＶＤドライブ３００を介してユーザ端末６００に接続される。ユーザ端末６００のＣＰＵ６１０は、ＤＶＤ－ＲＯＭ５００に記録されている暗号化済み映像コンテンツ５０３を読み出して表示装置６３０に表示する。

【００４２】ＤＶＤ－ＲＯＭ５００の通常のデータ格納領域には、正規ユーザ認証プログラム５０１、暗号解除プログラム５０４及び暗号化済み映像コンテンツ５０５が格納されている。認証プログラム５０１及び暗号解除プログラム５０４は、暗号化済み映像コンテンツ５０５を再生する際にＣＰＵ６１０により実行されるプログラムである。

【００４３】なお、ＢＣＡ領域５０に格納される識別情報５１及び正規ユーザ認証プログラム５０１を用いたユーザ認証動作については第１の実施形態と同様とし、ここでは詳細な説明を省略する。

【００４４】以下、図８のフローチャートを参照して、暗号化済み映像コンテンツの再生時のＣＰＵ６１０の動作について説明する。ＣＰＵ６１０は、正規ユーザ認証プログラム５０１に従って、まずＢＣＡ領域５０の識別情報５１を読み出す（Ｓ３００）。そして、読み出した識別情報５１に含まれるアプリケーション識別コードと認証プログラム５０１に記述されている正規のアプリケーション識別コードとを比較し（Ｓ３０２）、それらコードが一致するか否かを判定する（Ｓ３０４）。一致する場合にはオリジナルのディスクを使用する正規のユーザであると判断して暗号解除プログラム５０４に従って暗号化済み映像コンテンツ５０５を復号化して映像コンテンツを再生し（Ｓ３０６）、処理を終了する。一方、一致しない場合には、不正なユーザであると判断して暗号解除プログラム５０４を実行することなく処理を終了する。

【００４５】次に、以上の動作によって不正コピーによる映像コンテンツの不正利用が防止できることについて説明する。映像コンテンツは、ファイル単位で著作権保護が必要である。したがって、映像ファイルを不正コピーして利用することができないようにするためには、映像ファイルを暗号化しておく必要がある。暗号化した映像ファイルは、復号化しなければ利用することができない。そこで、本実施形態では、認証プログラム５０１によって、このメディアが不正コピーしたものではないオリジナルのメディアであると判断された場合のみ、この暗号化済み映像コンテンツ５０５を復号するための暗号解除プログラム５０４を有効化する。したがって、不正コピーされたメディアを再生することは不可能となる。

【００４６】なお、本実施形態では正規ユーザの認証にアプリケーション識別コードを用いたが、これに限らず、例えばＢＣＡ領域内の識別情報全体をキー情報として用いることも可能である。また、チェックデジットを用いた認証を行うことも可能である。

【００４７】また、本実施形態では正規ユーザ認証プログラム５０１と暗号解除プログラム５０４をそれぞれ独立したプログラムとして説明したが、これに限らず、暗号解除プログラム５０４が認証プログラム５０１の機能を含んでも構わない。

【００４８】また、本実施形態ではＤＶＤ－ＲＯＭ５００に記録される暗号化済み映像コンテンツ５０５は１つであったが、複数の映像コンテンツファイルをそれぞれ暗号化して記録しても構わない。

【００４９】以上のように、第３の実施形態によれば、映像コンテンツの再生時に、再生を行おうとする映像コンテンツの暗号化方式に対応した専用のデコーダ等を別途設けることなく暗号化済み映像コンテンツを再生することができるとともに、ＣＤキー等を手作業で入力することなしに正規ユーザの認証を行うことができるため認証作業が簡略化され、さらに、認証のためのキー情報として、書き換え不可能なＢＣＡ領域内の情報を利用しているため、不正コピーによる映像コンテンツの不正利用を防止することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るＤＶＤ－ＲＯＭを用いてソフトウエアプログラムをインストールする際のシステムの構成を示す図である。

【図２】第１の実施形態に係るＤＶＤ－ＲＯＭのＢＣＡ領域内の識別情報の構成の一例を示す図である。

【図３】第１の実施形態に係るＤＶＤ－ＲＯＭに記録されたソフトウエアプログラムのインストール時の動作を示すフローチャートである。

【図４】本発明の第２の実施形態に係るＤＶＤ－ＲＯＭを用いてインストールする際のシステムの構成を示す図である。

【図５】第２の実施形態に係るＤＶＤ－ＲＯＭのＢＣＡ領域内の識別情報の構成の他の一例を示す図である。

【図６】第２の実施形態に係るＤＶＤ－ＲＯＭに記録されたソフトウエアプログラムのインストール時の動作を示すフローチャートである。

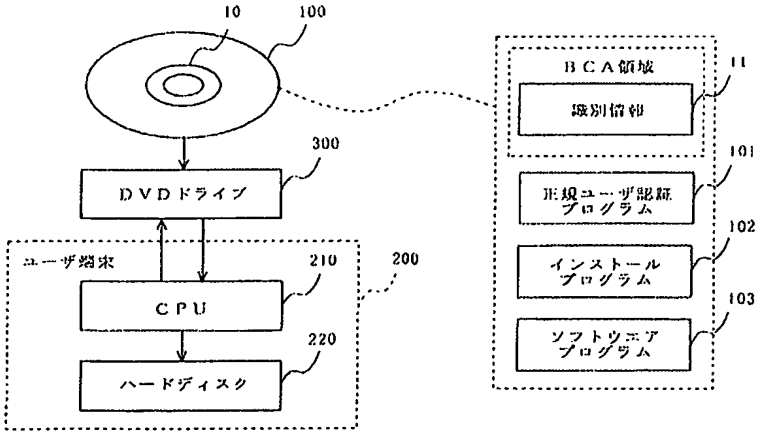
【図７】本発明の第３の実施形態に係るＤＶＤ－ＲＯＭを用いて映像コンテンツを再生する際のシステムの構成を示す図である。

【図８】第３の実施形態に係るＤＶＤ－ＲＯＭに記録された暗号化済み映像コンテンツの再生時の動作を示すフローチャートである。

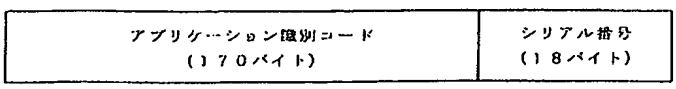
【符号の説明】

１０　ＢＣＡ領域
１１　識別情報
４０　ＢＣＡ領域
４１　識別情報
５０　ＢＣＡ領域
５１　識別情報
１００　ＤＶＤ－ＲＯＭ
１０１　正規ユーザ認証プログラム
１０２　インストールプログラム
１０３　ソフトウエアプログラム
２００　ユーザ端末
２１０　ＣＰＵ
２２０　ハードディスク
３００　ＤＶＤドライブ
４００　ＤＶＤ－ＲＯＭ
４０１　正規ユーザ認証プログラム
５００　ＤＶＤ－ＲＯＭ
５０１　正規ユーザ認証プログラム
５０４　暗号解除プログラム
５０５　暗号化済み映像コンテンツ

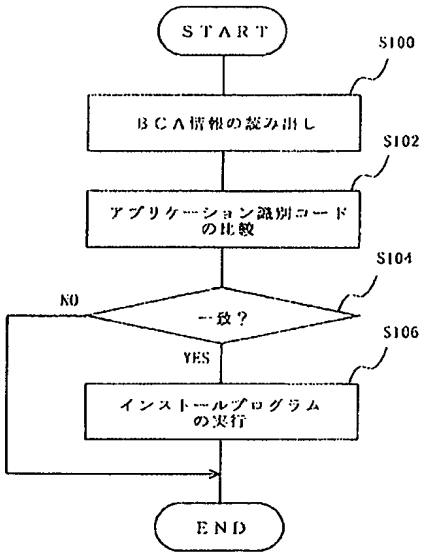
【図１】



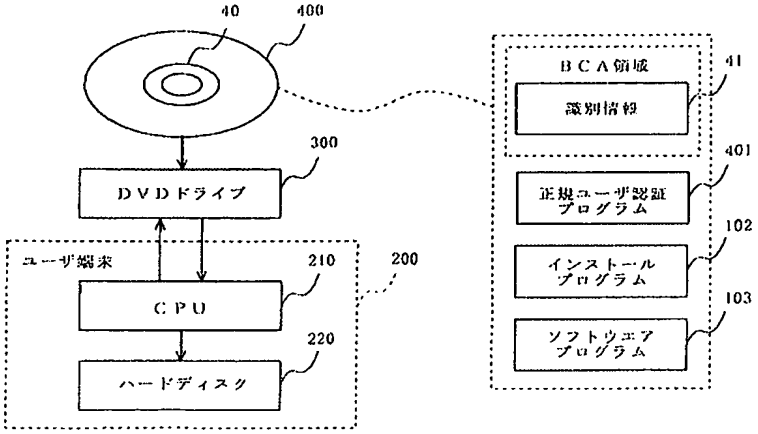
【図２】



【図３】



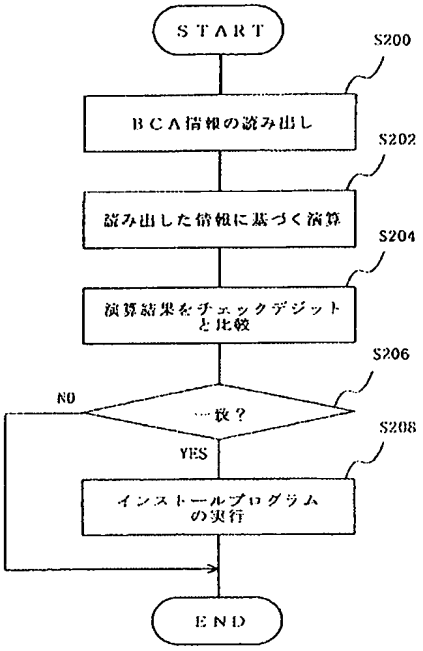
【図４】



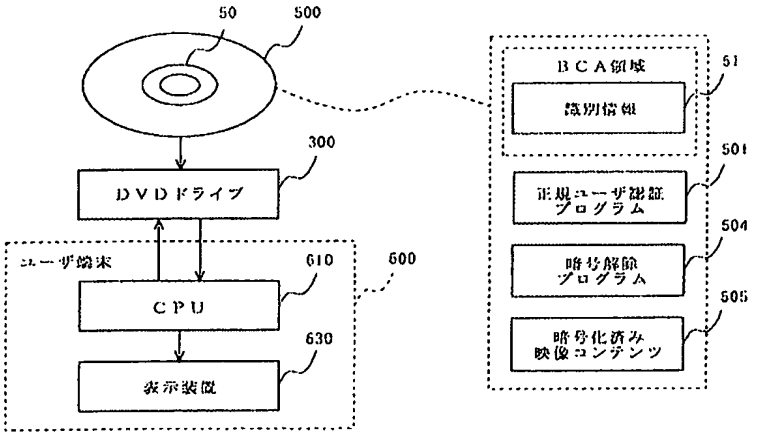
【図５】

アプリケーション識別コード（１６８バイト）	シリアル番号（１８バイト）	チェックデジット（２バイト）

【図６】



【図７】



【図８】